**网安学院2020级本硕博班靶机操作说明**

1. **组队**

同学们按自己意愿自行组队，4个同学一队，组完队后，选出一名队长，由队长将小组成员上报给指导老师。组队完成，指导老师为每个小组发布靶机和登录密码。

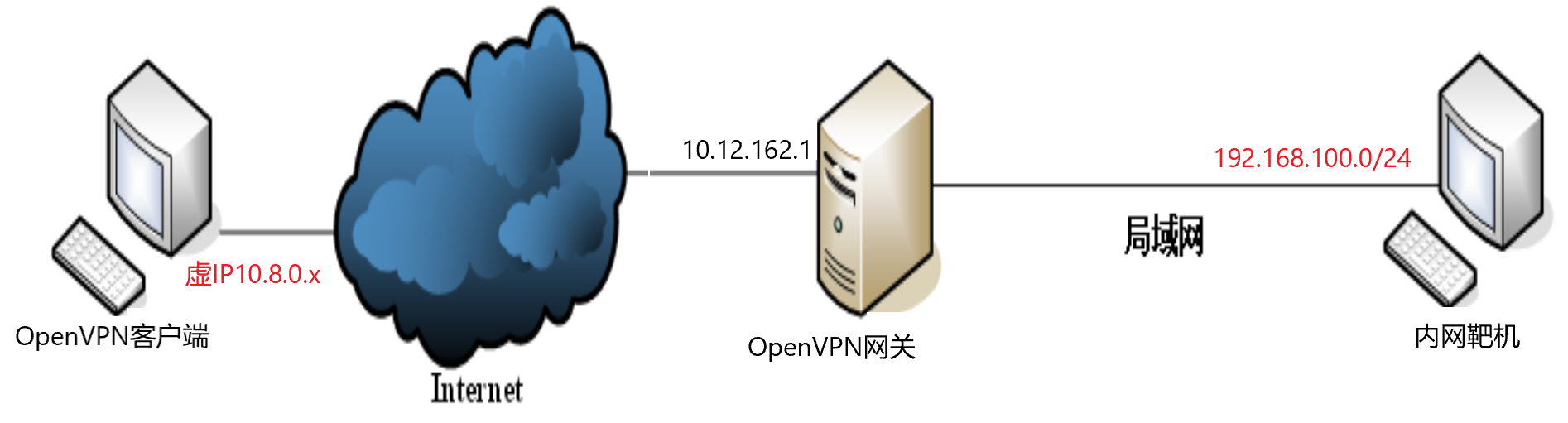
登录Cardinal平台提交flag账户/密码；登录靶机账号/密码。

1. **连接网络**

（1）安装openvpn，QQ群内有安装文件openvpn-install-2.4.8-I601-Win10，其他平台同学们可以自行在网上下载、安装。

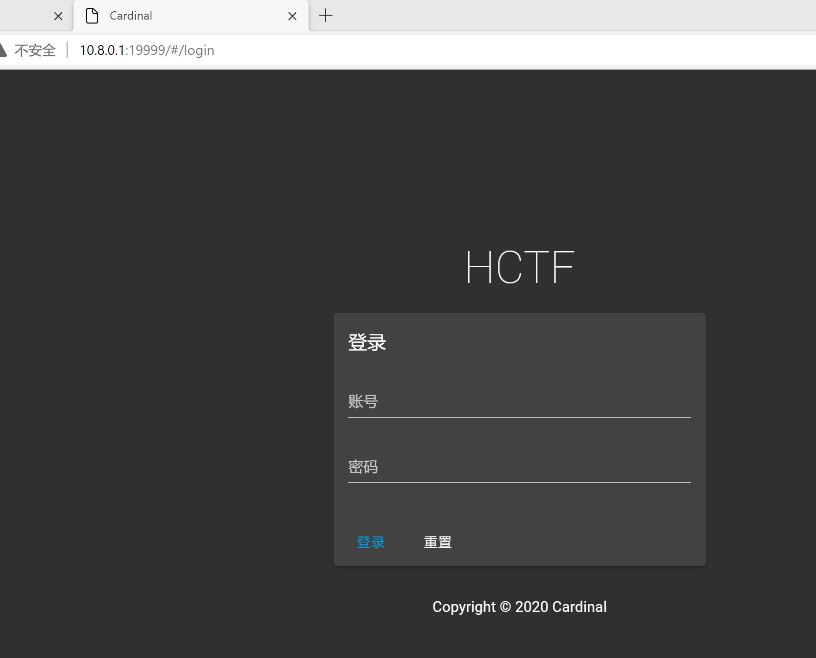
（2）将配置文件nccclient.ovpn拷贝到安装目录的config目录下，登录openvpn，用户名：user, 口令：cXf7qQAU8fwn1Ost。

**连接成功后，将成功建立一个10.8.x.x的虚拟网络。**



1. **获取任务**

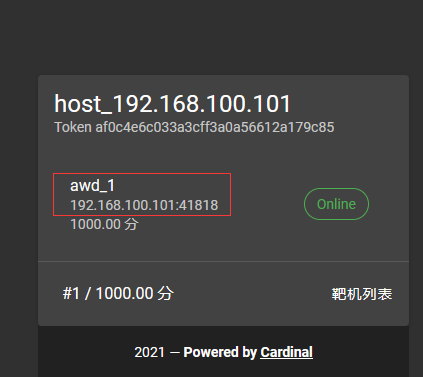
（1）浏览器访问<http://10.8.0.1:19999，(用户名>和密码由导师下发)，如下图所示。每个队伍公用一个用户名和密码。



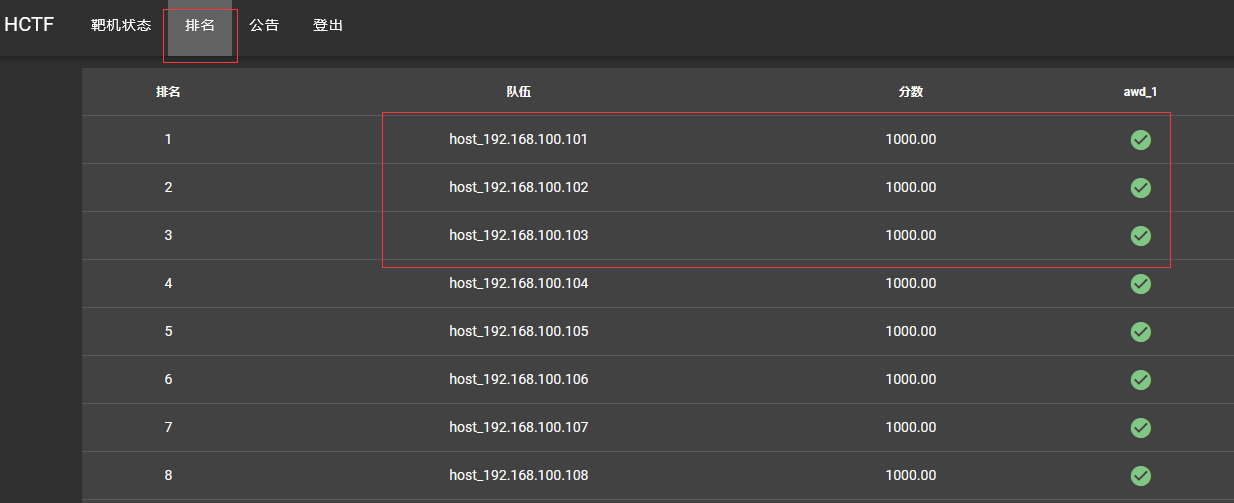
（2）查看自己的靶机的IP和WEB端口，下图**靶机列表中显示的靶机为各自队伍需要维护和防御的靶机（目前每个队伍只有一台靶机），其他靶机为攻击目标。**

**靶机模拟系统：** [**http://192.168.100.1\*\*:48180/**](http://192.168.100.1**:48180/)





（3）查看其他队伍的得分排名



（4）查看公告（略）

1. **AWD赛制介绍**

### [#](https://cardinal.ink/guide/rules.html#比赛开始) 比赛开始前

* 每个参赛选手均会拿到自己的比赛平台账号，从http://10.8.0.1:19999登录账号即可进入平台，可查看公告信息。
* 比赛开始前，选手无法查看自己的靶机信息。

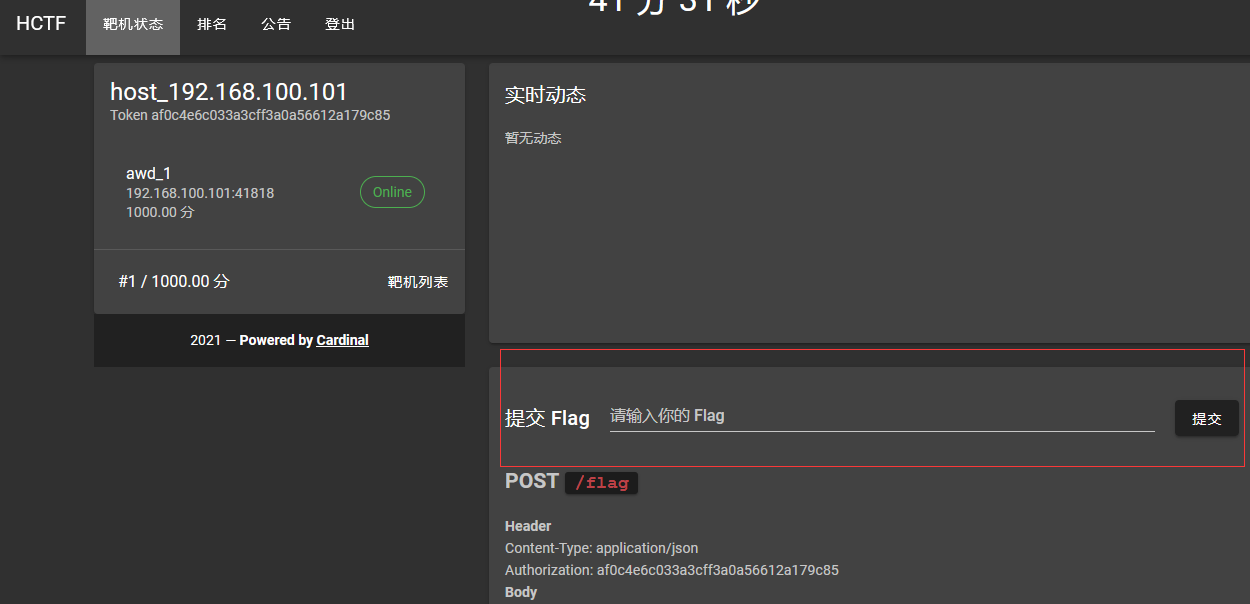
[**#**](https://cardinal.ink/guide/rules.html#比赛开始) **比赛开始**

* 选手可以查看自己的靶机信息，其中包括靶机的IP 地址，靶机 SSH 账号及密码(本此比赛将在公告中公布SSH账号密码)。
* 第一轮开始。

[**#**](https://cardinal.ink/guide/rules.html#新的一轮开始) **一轮进行中**

1. **攻击成功**

成功利用其他队伍靶机上的漏洞，获取到对方靶机上的 Flag 并提交，即攻击成功。此时，被攻击的队伍的靶机将显示为“被攻陷”状态。提交方式如下图：



例如将字符串，hctf{8db2582a045f6c3d5f622cebe4244cfb7265b2ba} 拷贝到横线处，点击“提交”按钮。如果成功，在排名中将会有所记录。

1. **被攻陷**

当靶机上的 Flag 被其他队伍提交时，该靶机将显示为“被攻陷”状态。

1. **被检测到服务宕机（CheckDown）**

当检测到靶机服务不可用或功能不全，则该靶机将显示为“宕机”状态。

**4.每轮时长60分钟。一台靶机在一轮中只会被攻陷一次（即最多只会被扣一次分）**

[**#**](https://cardinal.ink/guide/rules.html#一轮结束时) **一轮结束时**

* 结算上一轮各队伍得失分数，并更新排行榜。
* **新的一轮开始后，上一轮被攻陷的靶机如果没有防护，本轮仍然可以被攻击。**
* **每一轮的靶机中的Flag都是不同的。**

[**#**](https://cardinal.ink/guide/rules.html#比赛结束) **比赛结束**

* 完结撒花！
* 根据队伍最终排行榜排名，确定获奖情况。

[**#**](https://cardinal.ink/guide/rules.html#比赛结束)**分数结算规则**

这里假设攻击失分为 50 分，宕机失分为 50 分，每台靶机初始2000分。

* **被攻击失分**

被攻击的靶机，将减去 50 分。

* **攻击得分**

在该轮中成功攻击该靶机的所有队伍，一起平分该靶机扣分时失去的的分数。得分加到各自相应题目的靶机上。

例如：John 攻击了 Alice 的 Web1 靶机；Mashiro 攻击了 Alice 的 Web1 靶机。则 Alice 的 Web1 靶机 -50 分。John 和 Mashiro 各自的 Web1 靶机平分这减去的 50 分。即 John 和 Mashiro 每人 +25 分。此时全部队伍的加分与扣分之和，依然为零。

* **宕机（CheckDown）失分**

被 Check 检测到服务宕机的靶机，将减去 50 分。

* **服务正常得分**

在该轮中题目服务正常的靶机，平分该题目下，所有宕机靶机失去的分数。例如：John、Alice、Mashiro 的 Pwn2 靶机被检测判定为服务宕机，Asuna、Emiria 的 Pwn2 靶机一直服务正常。则 John、Alice、Mashiro 的 Pwn2 靶机各 -50 分。Asuna 和 Emiria 的 Pwn2 靶机平分这减去的 150 分。即 Asuna 和 Emiria 每人各 +75 分。此时全部队伍的加分与扣分之和，依然为零。

* **队伍总分**

队伍的所有靶机分数之和，即为队伍的总分数。排行榜按照队伍的总分数进行排名。

* **申诉**

出现系统误判的，可以找各班指导教师申诉，手工修改分数。

1. **本此比赛限制**

违反以下规则一旦被系统检测到将视同“宕机”：

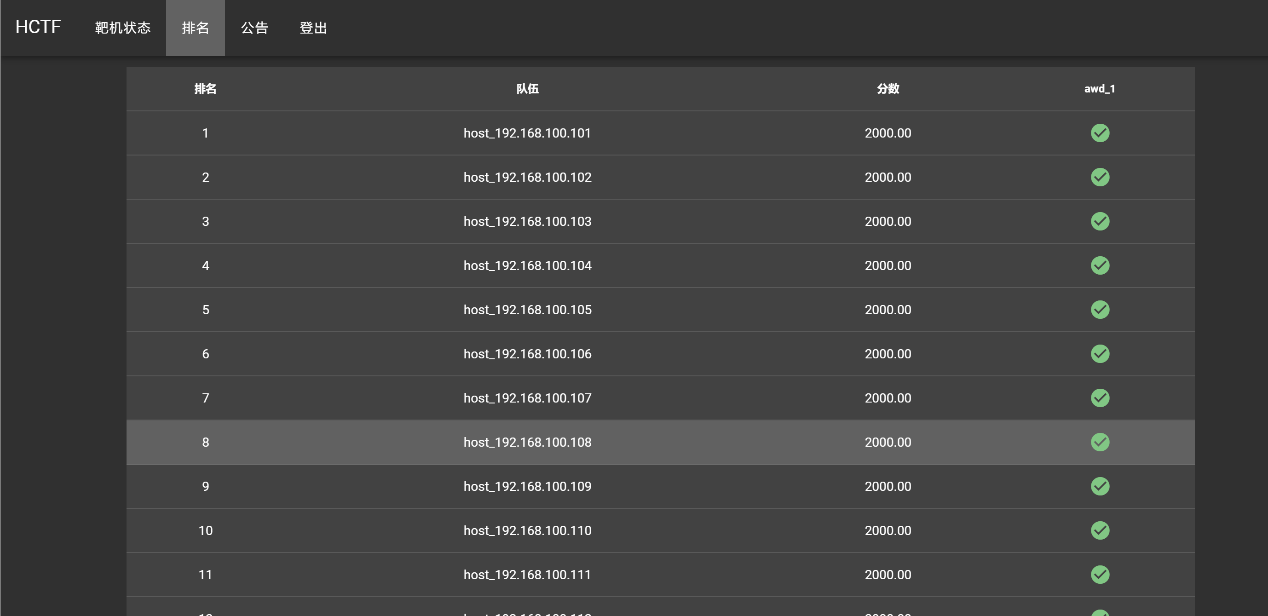
（1）修改应用程序导致WEB服务不能正常服务；

（2）修改或者删除机器中设置的Flag文件或者记录，或者恶意阻止平台对Flag更新，妨碍比赛公平性；

（3）恶意消耗宿主机磁盘空间导致系统故障。

**\*\*\*每天上课时间可以登录**[**http://10.8.0.1:/19999**](http://10.8.0.1:/19999)**提交Flag,课后Flag提交系统将关闭，各靶机仍然在线。**

**可以查看所有队伍排名情况。**

****

**可以查看系统公告**

****